**INTRODUCTION**

With the spread of technology and the penetration of the internet into every aspect of daily life, cyber security has begun to be of great importance for both individuals and states alike [1]. Although these innovations have made our lives easier, the increase in cyber attacks has made it necessary to take measures in this area [2]\_[4]. In addition, one of the most basic points is that the types of cyber attack, in other words the malicious use of cyberspace, have changed in the last 20 years. This has led to the use of new ``cyber'' concepts and risks in the literature [5].

A cyber attack is defined by Hathaway *et al.* as follows: ``A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose'' [6]. The most basic question to ask is `Does this definition define cyber attacks today?' Today, saying that cyberattacks are carried out only for political purposes is insufficient when it comes to trying to understand the nature of cyber attacks. This is because new cyber concepts have emerged that have changed the nature of cyber attacks. What remains similar is the use of computers in attacks. In this context, cybercrimes are defined as crimes committed through computers [7]. The Department of Justice of the USA defines a cybercrime as ``any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecution'' [8].

On the one hand, it is important to explain what cyber security is. Although the concept does not have any common definition, the International Telecommunication Union (ITU) defines cyber security as ``the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment'' [9].

Although there are now more complex structures in cyber attacks and cyber security compared to the past, the ability to perform cyber attacks has developed. The capacity to learn through websites that almost every computer user can access has increased. This is especially so the new generation, called the Z generation. They are often completely involved with computer technologies and can easily perform any activity they want by using it [10]\_[13].

On the other hand, this situation has also led to the emergence of new situations regarding computer technologies, or cyber security awareness as it is called in the literature. Although the Z generation has grown up with the internet and with computer technologies, sometimes they do not know what kind of problems they may encounter or they do not know how to deal with the problems arising from the continual development of internet technologies [14], [15].

Cyber security awareness, or information security awareness, has become an important issue today. The number of studies on this subject, which affects every aspect of daily life, is increasing. First of all, defining cyber security awareness is

important to better gain a full understanding of the subject. Shaw *et al.* defined the concept as; ``the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels

of information security control to protect the organization's data and networks'' [16]. As can be understood from the definition, the important points are evaluated in two ways. Firstly, it emphasizes the importance and responsibilities to do with information security. Secondly, it is aimed at knowing and applying information security control practices at an adequate level to protect the information.

Hwang *et al.* defined information security awareness as a phenomenon that aims to enable users to recognize the security vulnerabilities or problems that may arise and to respond in an appropriate way. Naturally, it also intends to keep the security phenomenon on the internet at the forefront of the user's minds [17]. Khan *et al.* made similar points to Hwang. Khan *et al.* defined information security awareness as the fact that users have information about security and act within the framework of the known rules [18]. Zilka, on the other hand, defines cyber security awareness as a phenomenon that aims to increase the level of knowledge about the online applications that users use so then they can stay safe in response to online risks [19]. Within the framework of these definitions, it can be clearly seen that security awareness training should be provided to improve cyber security awareness [20].

Within the framework of this information, it will also be questioned what kind of information the students have about cyber security awareness during the online education period and whether they want to receive training in this direction. The second aim of this study is to obtain data for use by further studies on how students can increase their cyber security awareness based on the theoretical framework findings.